What is DORA?

As of January 17, 2025, European Union (EU) financial entities and ICT third-party service providers designated as “critical” by the European Supervisory Authorities must be ready to comply with the EU Digital Operational Resilience Act (Regulation (EU) 2022/2554 - ‘DORA’). DORA standardizes how financial entities report cybersecurity incidents, test their digital operational resilience, and manage ICT third-party risk across the financial services sector and EU member states.

In addition to establishing clear expectations for the role of ICT providers, DORA will provide European Supervisory Authorities (ESAs) with direct supervisory powers over designated critical ICT providers. Microsoft is preparing to be designated as a “critical ICT third-party service provider” and will both comply with provisions under DORA, as applicable, and help regulated financial institutions meet their own requirements as well.

Regulatory Framework:

DORA aims to provide a harmonized approach to achieving "a high level of digital operational resilience" of the financial services industry (FSI) by ensuring that firms can withstand and adapt to a wide range of threats and disruptions, including cyber-attacks, IT failures, and other operational risks. DORA applies to a wide range of FSI entities, including banks, insurance institutions, stock exchanges, and trading platforms. It also, for the first time, will designate "critical ICT third-party service providers" or CTPPs deemed critical to the financial system by providing critical services to FSI entities, resulting in direct regulatory supervision of such designated firms.

Key Points to Consider:

1. **DORA's Purpose:** DORA seeks to enhance the resilience and stability of the FSI sector by ensuring that FSI entities have in place effective measures to manage and mitigate operational risks, including cyber risks. It aims to protect consumers, investors, and the wider FSI system from the potentially severe consequences of major disruptions or failures within the sector.
2. **Scope:** DORA applies to FSI entities operating in the European Union and to their ICT third-party providers who provide services in the EU, regardless of where the latter operate from. It also applies to Critical Third-Party Providers (CTPPs) designated by the ESAs, entrusted to the daily oversight of one of the three ESAs, i.e., either EBA, EIOPA, or ESMA.
3. **Key Provisions:** DORA includes primarily three requirements: (i) requirements applicable to FSI entities (including in areas of ICT Risk Management, notification of major ICT incidents, and operational resilience testing (i.e.,Threat Led Penetration Testing), (ii) requirements in relation to the contractual arrangements concluded between designated ICT third-party service providers and FSI entities, and (iii) rules for the establishment and conduct of the Oversight Framework for Critical ICT Third-Party Providers (CTPPs) when providing services to FSI entities.
4. **Compliance:** Microsoft will comply with all laws and regulations applicable to it in the provision of its services, subject to requirements as applied to it as a CTPP. FSI entities that have in place contractual arrangements for the use of Microsoft online services to run their critical or important functions shall remain accountable for compliance with all obligations under DORA and the applicable financial services regulatory requirements. Microsoft will support FSI entities to enable their compliance obligations and comply with the requirements applicable to it.
5. **Cloud Services and Providers:** DORA is technology neutral, and the requirements under DORA apply not only to FSI entities, but also to third party providers of ICT services who are designated as CTTPs. Certain Microsoft Azure cloud services (e.g., IAAS) and certain Microsoft 365 services such as Exchange and Teams are likely to be covered under DORA, though this is not yet determined.

6. **Contractual Commitments:** DORA mandates certain contractual requirements between the ICT third-party service providers and FSI entities. Microsoft will ensure its contractual provisions are in alignment with the requirement under DORA, as appropriate. Further, Microsoft already aligns to the requirements issued under EBA, ESMA and EIOPA guidance – and such guidance itself serves as a baseline framework for the requirements under DORA.
7. **Oversight:** DORA does not alleviate FSI entities from oversight of technology providers, including on audits. Microsoft has substantial experience supporting customers in executing on audits and in providing a level of transparency and assurance for continuous oversight and monitoring of its cloud services.

Conclusion:

DORA aims to strengthen the operational resilience of the FSI sector and seeks to bolster risk management so that firms can withstand and adapt to a wide range of threats and disruptions. Microsoft will comply with all laws and regulations applicable to it providing its cloud services, subject to requirements as applied to it as a CTTP. FSI entities that have in place contractual arrangements for the use of ICT third-party services shall remain accountable for compliance with all obligations under DORA and the applicable financial services regulatory requirements, to which Microsoft will support as required.

Primary Areas for Customers to Consider Under DORA

1. ICT Risk Management Framework

Requirements for EU financial entities: DORA establishes a comprehensive management mechanism of ICT risks with which financial entities would be required to comply—including the identification, protection and prevention, detection, response, and recovery of such risks in scope. Financial entities must establish an internal governance and control framework for ICT risk management and engage in ongoing monitoring of ICT risks. These ICT risk management and monitoring requirements extend to the use of ICT services provided by third party providers.

The elements of this ICT Risk Management Framework broadly encompass the following:

- **Internal governance and control framework for ICT risk management:** Financial entities must have an internal governance and control framework that ensures effective and prudent management of ICT risk.
- **ICT risk management framework components and requirements:** The ICT risk management framework must include strategies, policies, procedures, ICT protocols and tools that are necessary to protect and ensure the resilience, continuity and availability of ICT systems, information assets and data.
- **ICT systems, protocols, and tools specifications:** Financial entities must use and maintain updated ICT systems, protocols and tools that are appropriate, reliable, resilient, and capable of processing the data necessary for their activities and services. They must also implement ICT security policies, procedures, protocols, and tools that aim to ensure the security of networks and data and prevent ICT-related incidents.
- **Identification of ICT risk sources and dependencies:** Financial entities must identify, classify, and document all ICT supported business functions, information assets and ICT assets, and their roles and dependencies in relation to ICT risk. They must also identify all sources of ICT risk, cyber threats, and ICT vulnerabilities, and assess the potential impact of ICT disruptions.
- **Detection of ICT-related incidents and anomalies:** Financial entities must have mechanisms to promptly detect anomalous activities, ICT network performance issues and ICT-related incidents, and to identify potential single points of failure. They must also define alert thresholds and criteria to trigger and initiate ICT-related incident response processes.

- **Response and recovery from ICT-related incidents:** Financial entities must have a comprehensive ICT business continuity policy and associated ICT response and recovery plans that aim to ensure the continuity of critical or important functions, quickly and effectively resolve ICT-related incidents, and minimize damage and losses. They must also test, review, and update their plans and measures regularly, and report to the competent authorities as required.

How Microsoft Will Help

Microsoft already provides a broad set of built-in ICT risk management capabilities in our services today. This includes, by way of example: Microsoft Defender for Cloud, Microsoft 365 Service Health Dashboard, Microsoft Secure Score, Azure Service Health, and Microsoft Purview.

2. ICT - Related incident management, classification, and reporting

Requirements EU financial entities: A range of requirements are mandated on ICT incident management, classification, and reporting, including the following:

- **ICT-related incident management process:** Financial entities must have a process to detect, manage and notify ICT-related incidents and record them according to their priority and severity.
- **Classification of ICT-related incidents and cyber threats:** Financial entities must classify ICT-related incidents and cyber threats based on criteria such as the number of clients affected, the duration, the geographical spread, the data losses, the criticality of the services and the economic impact.
- **Reporting of major ICT-related incidents and voluntary notification of significant cyber threats:** Financial entities must report major ICT-related incidents to the relevant competent authority using standard forms and templates and inform their clients about the incident and the mitigation measures. Financial entities may also notify significant cyber threats to the relevant competent authority on a voluntary basis.
- **Harmonization of reporting content and templates:** The ESAs, through the Joint Committee, and in consultation with ENISA and the ECB, shall develop common draft regulatory and implementing technical standards to specify the content, the time limits and the format of the reports and notifications for ICT-related incidents and cyber threats.
- **Centralization of reporting of major ICT-related incidents:** The ESAs, through the Joint Committee, and in consultation with the ECB and ENISA, shall prepare a joint report assessing the feasibility of further centralizing incident reporting through the establishment of a single EU Hub for major ICT-related incident reporting by financial entities.

How Microsoft Will Help

Microsoft provides such capabilities to support on incident management with services such as Microsoft Defender. Further, Microsoft 365 Compliance Center and Azure Sentinel provide tools and capabilities for efficient incident detection, investigation, reporting, and management, aligning with regulatory requirements for timely incident reporting and response. Further, Microsoft will make available updated contract terms as required under DORA, including in relation to ICT-Related Incidents. Further, Microsoft will address and assist, as needed, other requirements under DORA and work with industry stakeholders accordingly.

3. Digital operational resilience testing

DORA introduces digital operational tests that should be conducted on critical ICT systems and applications on an annual to triennial basis through threat-led penetration testing (TLPT). This new testing approach will bolster the testing capabilities of financial entities—fostering timely recovery and business continuity. Microsoft already enables customers to do so through our penetration testing program. Learn more about the Microsoft Cloud Penetration Testing Rules of Engagement and our Bug Bounty programs. Microsoft will further work through and support testing requirements to meet the requirements under this testing regime as required under DORA, consistent with principles of ensuring the safety, integrity, security, and operational resilience of the Microsoft Cloud.

4. Key principles for a sound management of ICT third-party risk

Requirements of Financial Entities: Financial entities will be expected to manage ICT third-party risk as part of their ICT risk management framework, adopt a strategy and a policy on the use of ICT services supporting critical or important functions, and maintain a register of information on all contractual arrangements with ICT third-party service providers.

- **Preliminary assessment before entering into contracts:** Financial entities should assess the risks of contracting with key ICT third-party service providers.
- **Key contractual provisions:** Financial entities should ensure that the contractual arrangements include, among other things, a description of the functions and services, the locations of data processing and storage, management and supervision of key subcontractors that underpin the provision of critical services, the data protection and security measures, the service level descriptions and performance targets, the termination rights and exit strategies, and the access, inspection and audit rights of the financial entity and the competent authorities.

How Microsoft Will Help

Microsoft already provides substantial contractual commitments that are in alignment with the guidance from the respective ESAs and consistent with the provisions under Article 30 of DORA. Microsoft Data Protection Addendum, Product and Service Terms and Financial Services Amendment cover these key elements. We will work with customers to continue to address further customer needs going forward.

5. Microsoft's Commitment to Enable Compliance Under DORA

Microsoft is preparing to meet the requirements under DORA, as applicable to it, and the key services it provides to financial entities that use its cloud services for critical or important functions. Microsoft has for over a decade invested significantly into helping financial institutions meet their regulatory obligations when using Microsoft cloud services – from the commercial contracts we make available consistent with ESAs guidelines on outsourcing, to transparency and assurance of our cloud services through the Service Trust Portal and other resources, to the myriad of built-in security features in our cloud services. Coupled with the breadth of capabilities we offer to help customers manage risk and oversee use of our cloud services on a continuous basis, the elements of DORA are a natural step forward to maintain operational resilience and use Microsoft cloud services with confidence. We are also working with other regulators in jurisdictions such as the UK that are implementing similar measures as DORA and are preparing to meet those requirements as well.